

## Asymmetrische Kryptographie

Im Rahmen der Überlegungen zum Übungsblatt „symmetrische Kryptographie“ wurde deutlich, dass die Verteilung von Schlüsseln eine große Herausforderung darstellen kann.

In den Jahren von 1970 bis 1978 wurden dann, für den damaligen Kenntnisstand der Kryptographie, revolutionäre neue Verfahren erdacht, die eine Lösung für das Problem der Schlüsselverteilung versprachen. Diese Verfahren sind heute unter den Begriffen „**Asymmetrische Kryptographie**“ oder auch „**Public-Key-Kryptographie**“ bekannt.

Die Grundidee besteht darin, nicht mehr denselben Schlüssel für das Ver- und Entschlüsseln zu verwenden, sondern Schlüsselpaare. Ein Schlüssel wird nun dazu verwendet die Nachricht zu verschlüsseln und der andere (dazugehörige) Schlüssel dazu, die Nachricht wieder zu entschlüsseln.

Zu einem Schlüsselpaar gehören also zwei Schlüssel, die miteinander in einer mathematischen Beziehung stehen, aber nicht voneinander abgeleitet werden können. D.h. kennt man einen der beiden Schlüssel so kann einem der andere, der dazugehörige, auch völlig unbekannt bleiben.

Jeder Teilnehmer an einer Public-Key-Infrastruktur verfügt nun über ein Schlüsselpaar. Einen davon, den sogenannten öffentlichen Schlüssel macht er dabei allen anderen Teilnehmern bekannt – den zweiten Schlüssel, seinen privaten Schlüssel, hält er streng geheim und benutzt ihn ausschließlich selbst.

Eine verschlüsselte Kommunikation könnte nun wie folgt ablaufen:

1. Alice macht Bob Ihren öffentlichen Schlüssel bekannt
2. Bob benutzt diesen Schlüssel (also den öffentlichen Schlüssel von Alice) um seine Nachricht an Alice zu verschlüsseln
3. Alice benutzt Ihren geheimen Schlüssel um die Nachricht, die Bob zuvor mit Ihrem öffentlichen Schlüssel verschlüsselt hat zu entschlüsseln. Da nur Sie Ihren privaten Schlüssel kennt, und nur dieser Schlüssel dazu geeignet ist die Nachrichten von Bob zu entschlüsseln, kann nur Alice die Nachricht dechiffrieren.

### Aufgabe 1:

Erzeugen Sie zunächst mit OpenSSL ein Schlüsselpaar. Gehen Sie dabei wie folgt vor:

Erzeugen Sie zuerst mittels der Eingabeaufforderung Ihren privaten Schlüssel. Geben Sie dazu das folgende Kommando ein:


```
openssl genrsa -out private.pem 2048
```

Erzeugen Sie anschließend, den dazugehörigen öffentlichen Schlüssel:

```
openssl rsa -in private.pem -pubout > public.pem
```

Sehen Sie sich die erzeugten Dateien private.pem und public.pem in einem Texteditor an.

„Veröffentlichen“ Sie Ihren **öffentlichen Schlüssel** auf dem Tauschlaufwerk (Ordner PublicKeys) und geben Ihrer Schlüssel-Datei public.pem einen „sprechenden“ Namen wie z.B. FritzchenMuellerPublic.pem

	Kryptographie	it.schule stuttgart Breitwiesenstrasse 20-22 70565 Stuttgart
	Übung – Asymmetrische Kryptographie	

### **Aufgabe 2:**

Wählen Sie einen Empfänger und verschlüsseln Sie eine „geheime“ Nachricht. Gehen Sie dabei wie folgt vor:

Erzeugen Sie mit einem Texteditor eine Textdatei mit Ihrer **kurzen** geheimen Nachricht „geheim.txt“.

Danach verschlüsseln Sie die Textdatei unter Verwendung des öffentlichen Schlüssels des Empfängers mit dem Befehl:

```
openssl rsautl -encrypt -inkey FritzchenMuellerPublic.pem -pubin -in geheim.txt -out geheim.enc
```

Die Aufgabe gilt als erfolgreich absolviert, wenn es dem Empfänger gelingt Ihre Nachricht mit dem folgenden Befehl zu entschlüsseln:

```
openssl rsautl -decrypt -inkey private.pem -in geheim.enc -out geheim.txt
```

### **Aufgabe 3:**

Kopieren Sie sich vom Tauschlaufwerk die (relativ große Datei): einFilm.avi

Verschlüsseln Sie die Datei (einFilm.avi) zunächst symmetrisch mit dem Befehl:

```
openssl enc -e -aes256 -in einFilm.avi -out einFilm.avi.enc
```

Versuchen Sie nun die Datei einFilm.mpeg4 mit dem Befehl:

```
openssl rsautl -encrypt -inkey public.pem -pubin -in einFilm.avi -out einFilm.avi.enc
```

asymmetrisch zu verschlüsseln.

Welche Erfahrung machen Sie?